

REMARKS

Allowable Subject Matter

Applicant wishes to thank the Examiner for indicating that claims 12 and 13 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claim. Claims 12 and 13 have been so amended.

Claim Rejections 35 USC §103

Claims 1-3 and 6-10 have been rejected under 35 USC §103 as being unpatentable over Nachenberg '008 in view of Nachenberg '057 and in further view of Schmall.

The Nachenberg references describe viruses (suspect computer programs) that are encrypted and thus that must be transformed into a non-encrypted version before signature detection. After decryption, the viruses are scanned, apparently using a standard string comparison, against a virus definition file. See, for example, column 7, lines 30-37.

This preprocessing of the virus to decrypt it is believed to be distinguishable from the generation of a "logically equivalent standardized version" of the virus as would be required by the present claims which contemplates that both the "suspect computer program" and its "logically equivalent standardized version" are executable programs (permitting them to be logically equivalent when executed on a computer). Claim 1 has been amended to more clearly indicate that the "logically equivalent standardized version" and the "suspect computer program" are both in executable form and one not simply the decryption of an encrypted program, the latter which could not be executed as encrypted or if executed would not result in a logically equivalent execution. This point is emphasized with an additional amendment to claim 1 indicating that the meaning of the "logical equivalent standardized version" is that it would execute produced the same result as the "suspect computer program".

Based on this amendment, it is believed that the Nachenberg references, even in combination, fail to teach the claimed preprocessor of the present invention which takes a suspect computer program and creates a logically equivalent standardized version of that suspect computer program.

Schmall, which is cited primarily for the proposition of creating the "logically equivalent standardized version" without execution of the suspect program (Nachenberg require execution

or emulation of the viral code to decrypt it) does not appear to remedy the deficiencies of the Nachenberg references. Schmall appears to work by analyzing statistical occurrences of certain types of instructions in the viral code as recorded by flags. See, for example, column 4, line 65 to column 5, line 19. The number of occurrences of particular types of instructions are then analyzed to indicate a statistical likelihood of a virus. It is believed that this process of generating flags and analyzing them does not create a "logically equivalent standardized version" of the virus program, but in any case does not produce a program in executable form that would execute to produce the same result as the suspect program.

In light of these amendments, it is believed that claim 1 is also now in condition for allowance together with the remaining claims 2-10 and 14-17 dependent on claim 1, and claims 11 and 12, amended to be in independent form as described above. Applicants appreciate consideration of the above remarks and invite the Examiner to telephone the undersigned in the event a telephone discussion would be helpful in advancing the prosecution of the present application. The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-1170.

Respectfully submitted,

CHRISTODORESCU, ET AL

A handwritten signature in black ink, appearing to read 'Keith M. Baxter', is written over a horizontal line. The signature is stylized with a large loop at the end.

By _____

Keith M. Baxter
Reg. No. 31,233
Attorney for Applicant
Boyle Fredrickson
840 North Plankinton Avenue
Milwaukee, WI 53203